



## EVKLIDOV ALGORITEM

Definicija: Za vsak  $a \in \mathbb{Z}$  in  $b \in \mathbb{N}$  obstajata naravnih deliteljev  $g$  in  $r$ ,  $0 \leq r < b$ , da velja  $a = gb + r$ .

Z Evklidovim algoritmom imemo naprej skupni delitelj d števil  $a$  in  $b$ , e razširjen EA pa tudi  $x$  in  $y$  s  $ax + by = d$ .

$$\text{Reši } 4928x - 1771y = \gcd(4928, 1771)$$

$$4928 = 2 \cdot 1771 + 1386$$

$$4928x - 1771y = 77 \quad | : 77$$

$$1771 = 1 \cdot 1386 + 385$$

$$64x - 23y = 1$$

$$1386 = 3 \cdot 385 + 231$$

$$64 = 2 \cdot 23 + 18$$

$$385 = 1 \cdot 231 + 154$$

$$23 = 1 \cdot 18 + 5$$

$$231 = 1 \cdot 154 + 77$$

$$18 = 3 \cdot 5 + 3$$

$$154 = 2 \cdot 77 + 0$$

$$5 = 1 \cdot 3 + 2$$

$$\hat{=} \gcd(4928, 1771)$$

$$3 = 1 \cdot 2 + 1$$

$$1 = 3 - 2 = 3 - (5 - 3) = 2 \cdot 3 - 5 = 2(18 - 3 \cdot 5) - 5 = 2 \cdot 18 - 7 \cdot 5 =$$

$$= 2 \cdot 18 - 7 \cdot (23 - 18) = 9 \cdot 18 - 7 \cdot 23 = 9 \cdot (64 - 2 \cdot 23) - 7 \cdot 23 =$$

$$= 9 \cdot 64 - 25 \cdot 23 \quad x_0 = 9 \quad y_0 = +25$$

$$x = 9 + 23k \quad y = +25 + 64k, \quad k \in \mathbb{Z}$$

Dokaz, da 77 deli 4928 in 1771, premo od spodaj narezen po metodici.

Tedno je EA konča, ker se ostanele na vatem koraku enačba

vrij ena 1, in pravkar je isti konakov logaritemsko odvisen od velikosti  $b$ .

# LINEARNA DIOFANTSKA ENAČBA



$a, b, c \in \mathbb{Z}$  dani, iščemo  $x, y$  za  $ax + by = c$

Racionalne rešitve so „ber vere“:  $y = \frac{c - ax}{b}$ . Oti iščemo cele rešitve:  $x, y \in \mathbb{Z}$ .

Diofantiske enačbe: polinomske enačbe s celimi koeficienti; na hiter iščemo celoštevilске rešitve (linearne DE, Pitagoripke trojice, Pellova enačba...)

Rešitev linearne DE obstaja  $\Leftrightarrow$  največji skupni delitelj  $a$  in  $b$  deli  $c$ . Kar mora  $a$  in  $b$  skupnega, mora imeti tudi  $c$ .

Če imamo eno rešitev  $x_0, y_0$ , ostale dobimo kot

$$x = x_0 - \frac{b}{d}k, \quad y = y_0 + \frac{a}{d}k, \quad d = \text{D}(a, b), \quad k \in \mathbb{Z}$$

$$\text{D}: a(x_0 - \frac{b}{d}k) + b(y_0 + \frac{a}{d}k) = c \rightarrow ax_0 + by_0 - \frac{ab}{d}k + \frac{ab}{d}k = c$$

Če velja  $a(x_0 + u) + b(y_0 + v) = c$ , je  $au = -bv$  in  $av = -bu$ ,  $a, b$  tuja, zato  $v$  deli  $a_1 = \frac{a}{d}$ ,  $u$  deli  $b_1 = \frac{b}{d}$ ,  $v = b \cdot \frac{a}{d}$ ,  $u = -b \cdot \frac{a}{d}$ .

Rešitev  $x_0, y_0$  poisciemo z razširjenim Euklidovim algoritmom:

$$r_{-1} = a = 1 \cdot a + 0 \cdot b$$

Dobimo rekurzivni izraz

$$r_0 = b = 0 \cdot a + 1 \cdot b$$

$$x_{k+1} = x_{k-1} + g_{k+1} x_k$$

$$r_1 = 1 \cdot a - g_1 \cdot b$$

$$y_{k+1} = y_{k-1} + g_{k+1} y_k$$

$$r_2 = b - g_2 \cdot r_1 = b - g_2(a - g_1 b)$$

$$x_{-1} = 1, \quad x_0 = 0$$

$$r_3 = r_1 - g_3 \cdot r_2$$

$$y_{-1} = 0, \quad y_0 = 1$$

$$r_n = (-1)^{k-1} x_k a + (-1)^k y_k b$$



## PITAGOREJSKE TROJICE

Isčemo  $x, y, z \in \mathbb{Z}$ , ki rešijo  $x^2 + y^2 = z^2$ . Rešitev v

$\mathbb{Q}$  so ekvivalentne rešitve v  $\mathbb{Z}$ , saj  $\left(\frac{x_1}{z_2}\right)^2 + \left(\frac{y_1}{z_2}\right)^2 = \left(\frac{z_1}{z_2}\right)^2 / \cdot (z_1 z_2)^2$   
 $(x_1 y_1 z_2)^2 + (y_1 z_2 z_2)^2 = (z_1 x_2 y_2)^2$ . Dovolj bo najti primitive rešitve  $\rightarrow$  največji skupni delitelj  $x, y, z$  je 1. Blam jih lahko množimo s poljubnim celim številom.

I: Vse primitive Pitagorejske trojice so oblike

$x = t^2 - s^2, y = 2st, z = t^2 + s^2$ , s in t tudi naravnimi števili razlicne parnosti in  $s < t$ .

D: Pitagorejske trojice so ekvivalentne razionalnim točkam na enotni krožnici:  $x^2 + y^2 = z^2 \rightarrow \left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1$ , te pa razionalnim

koefficientom pravice skozi  $(1, 0)$ :  $k = \frac{n}{m+1} \in \mathbb{Q}$ . Izrazimo n in r s k:

$$n = km + m, \quad 0 = k(-1) + m, \quad m = k, \quad n = k(m+1), \quad m^2 + n^2 = 1 \rightarrow m^2 + k^2(m+1)^2 = 1$$

$$m^2 + k^2 m^2 + 2k^2 m + k^2 - 1 = 0 \quad m = -1 \text{ neri, tako } m^2(1+k^2) + 2k^2 m + k^2 - 1 = 0$$

$$(m+1)(m(1+k^2) + k^2 - 1) = 0 \quad m^2(1+k^2) + m^2 - m + m^2 k^2 + k^2 - 1 = 0$$

$$m = \frac{1-k^2}{1+k^2}, \quad n = k(m+1) = \frac{2k}{1+k^2}. \quad \text{Pisemo } k = \frac{2}{t} \text{ in dobimo}$$

$$m = \frac{s}{t} = \frac{t^2 - s^2}{t^2 + s^2}, \quad n = \frac{y}{t} = \frac{2st}{t^2 + s^2}. \quad \text{E bili s in t obe liki}$$

ali obe nudi, bi bila  $x, y, z$  vsa cela števila.

Za  $x^n + y^n = z^n$  ni (ne)trivialnih rešitev, če je  $n \geq 3$ .

Enačba  $x^4 + y^4 = z^2$  nima naravnih rešitev. (Temat)

Dokaz: Če imamo rešitev, imamo tudi strogo manjše rešitev, kar v  $\mathbb{N}$  ne gre v redogled.



## KONGRUENCE

$$a \equiv b \pmod{n} \Leftrightarrow a - b \mid n \Leftrightarrow a - b = k \cdot n \Leftrightarrow a = b + k \cdot n$$

$a$  in  $b$  dosta pri deljenju z  $n$  isti ostaneš.

$\mathbb{Z}_n = \{0, 1, \dots, n-1\}$  standardni popolni sistem ostankov, kar je grupa za restovanje in tudi bolobar (članek v delitljivosti).

$$T: a \equiv b \pmod{n}, c \equiv d \pmod{n} \Rightarrow a+c \equiv b+d \pmod{n}, ac \equiv bd \pmod{n}, a^k \equiv b^k \pmod{n}$$

ni tako bistveno

$$T: \bullet a \equiv b \pmod{n} \text{ in } d \mid n \Rightarrow a \equiv b \pmod{d} \quad 7 \equiv 17 \pmod{10} \Rightarrow 7 \equiv 17 \pmod{5} \quad (2)$$

$$\bullet a \equiv b \pmod{n_1}, a \equiv b \pmod{n_2}, \dots, a \equiv b \pmod{n_k} \text{ in } n_1 \text{ in } n_k \text{ paroma triji} \\ \Rightarrow a \equiv b \pmod{n_1 \cdot n_2 \cdots n_k} \quad a \equiv 5 \pmod{7} \text{ in } a \equiv 33 \pmod{51} \quad a \equiv 5 \equiv 33 \pmod{7} \Rightarrow a \equiv 33 \pmod{357}$$

$$\bullet ac \equiv bc \pmod{n} \text{ in je } d = (c, n) \Rightarrow a \equiv b \pmod{\frac{n}{d}} \quad 14 \equiv 20 \pmod{6} \text{ in } d(2, 6) = 2 \Rightarrow 7 \equiv 10 \pmod{3}$$

Linearna kongruenca:  $ax \equiv b \pmod{n}$   $a, b \in \mathbb{Z}, n \in \mathbb{N}$ , inamo

$\times$  1) Če je  $a$  trij modulu  $n$ , inamo matanko eno rešitev  $x \pmod{n}$ . 2) Če  $d = (a, n)$  deli  $a$  in  $n$ , ne pa tudi  $b$ , ni rešitev. 3) Če  $d = (a, n)$  deli tudi  $b$ , ina enačba  $d$  melkongruentnih rešitev mod  $n$  oblike  $x_0 + k \frac{n}{d}$ ,

$$k = 0, 1, \dots, d-1, \text{ kjer je } x_0 \text{ rešitev } \frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$$

$$D: 1) \text{ Ko } x \text{ priteče } \mathbb{Z}_n, \text{ tudi } ax \text{ priteče } \mathbb{Z}_n \text{ matanko enkrat.} \quad 2) \quad \begin{array}{c} \downarrow \text{mod } d \\ \downarrow \quad \downarrow \\ ax = b + k \cdot n \end{array}$$

$$3) \text{ Ko mod } \frac{n}{d} \text{ je matanko ena rešitev } x_0 \text{ in } ax_0 + k \frac{n}{d} = b + l \cdot n \quad \text{mecz}$$

Pozor: V primeru 3) ina enačba 1. stopnje neč bo eno rešitev

Sistemi:  $a_1x \equiv b_1 \pmod{n_1}, a_2x \equiv b_2 \pmod{n_2}, \dots, a_kx \equiv b_k \pmod{n_k}$  rešujemo jih

postopno (po običahu in sprotnosti). Če so si moduli paroma triji: Kitajski

izrek o ostankih: Sistem  $x \equiv c_i \pmod{n_i}$ ,  $n_i$  paroma triji, ima matanko eno rešitev mod  $N = n_1 \cdot n_2 \cdots n_k$  in je  $x \equiv \sum_{i=1}^k b_i N_i c_i \pmod{N}$ , kjer  $N_i = \frac{N}{n_i}$  in  $b_i N_i \equiv 1 \pmod{n_i}$ .



## EULERJEVA FUNKCIJA IN EULERJEV IZREK

Eulerjeva funkcija  $\varphi(n) = |\mathbb{Z}_n^*|$  je število elementov v  $\mathbb{Z}_n$ , ki so tuji n.  $\mathbb{Z}_n^*$  je reducirani sistem ostankov po modulu n. Je grupa za množenje.

$$\mathbb{Z}_{12}^* = \{1, 5, 7, 11\} \quad \varphi(12) = 4$$

Eulerjev izrek: Če je  $a \in \mathbb{Z}_n^*$  (a tuji n), je  $a^{\varphi(n)} \equiv 1 \pmod{n}$ .

D:  $\mathbb{Z}_n^*$  je grupa in moč je  $\varphi(n)$ , zato je vsak element na red grupe enak 1.

oz.  $\{g_1, g_2, \dots, g_{\varphi(n)}\} = \{ag_1, ag_2, \dots, ag_{\varphi(n)}\}$ . Množici zmnožimo modulom n:  
 $g_1 g_2 \dots g_{\varphi(n)} \equiv a^{\varphi(n)} \pmod{n}$  in  $g_1 g_2 \dots g_{\varphi(n)}$  se hrajojo, ker so tuji n.

Mali Fermatov izrek: p prastevilo,  $a \in \mathbb{Z}$ , ~~p ne delja~~, potem je  $a^{p-1} \equiv 1 \pmod{p}$ . D:  $|\mathbb{Z}_p^*| = p-1$  a ni včravniš p

Zivijo!

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{4}$$

$$x \equiv 4 \pmod{5}$$

$$x \equiv 1 \pmod{7}$$

$$140d \equiv 2 \pmod{3} \quad d \equiv 1 \pmod{3}$$

$$105c \equiv 3 \pmod{4} \quad c \equiv 3 \pmod{4}$$

$$84b \equiv 4 \pmod{5} \quad b \equiv 1 \pmod{5}$$

$$60a \equiv 1 \pmod{7} \quad a \equiv 2 \pmod{7}$$

$$\begin{aligned}
 x &= 3 \cdot 4 \cdot 5a + 3 \cdot 4 \cdot 7b + 3 \cdot 5 \cdot 7c + 4 \cdot 5 \cdot 7d \\
 &= 60a + 84b + 105c + 140d \\
 &= 3 \cdot 4 \cdot 5(7k+2) + 3 \cdot 4 \cdot 7(5l+1) + 3 \cdot 5 \cdot 7(4m+1) + \\
 &\quad + 4 \cdot 5 \cdot 7(3n+1) \\
 &= 120 + 84 - 105 - 280 + 3 \cdot 4 \cdot 5 \cdot 7(k+l+m+n) \\
 &\equiv -181 \pmod{420}
 \end{aligned}$$



## ŠIFRIRANJE

Sporočilo čelimo spremeniti tako, da ga nihče brez dodatnih informacij ne more razvredlati.

Zamenjalna šifra: abecedo zamaknemo oz. permutiramo inhe.  $f(x) = ax + b$  (sl. vklj. npr. 25)

Glabosti: Ohranili smo presledke in s tem dobro besed, zato lahko razvredlamo na podlagi frekvenc črk in naravnem jeziku. V slovenščini je 10% c-jev in 10% a-jev.

Tillovo šifriranje: besedilo razdelimo na bloke in jih preslikujemo z matrico  $A \in \mathbb{Z}_n^{k \times k}$ ,  $f(x) = Ax \pmod{n}$ , A mora biti obrnjiva v  $\mathbb{Z}_n$ , torej  $\det A \in \mathbb{Z}_n^*$

Eksponentna šifra:  $f(x) = x^e \pmod{p}$  in pod pogojem  $d(e, p-1) = 1$  imamo inverzno preslikavo  $f^{-1}(x) = x^d \pmod{p}$ ,  $ed \equiv 1 \pmod{p-1} \Rightarrow ed = 1 + k(p-1)$ .  
 $x^{ed} = x \cdot (x^{p-1})^k \equiv x \pmod{p}$  (mali Fermat). Pomembno je, da je ed=1 mod p-1, kar pomeni, da je ed=1 mod p-1. Pomevanje e in p-1 je primerno le za privatno komunikacijo.

RSA: eksponentna, le da za modul uporabljamo  $r = p \cdot q$  produkt dveh velikih praštevil, ki pa je celo težko razcepiti:  
 $f(x) = x^e \pmod{r}$   $g(y) = y^d \pmod{r}$ ,  $x^{cd} \equiv x \pmod{r}$ , vemo  $x^{q(r)} \equiv 1 \pmod{r}$  za  $x \neq r$ .  $ed \equiv 1 \pmod{\phi(r)}$ ,  $e \in \mathbb{Z}_r^*$ .  $d$  je inverz e po modulu  $(p-1)(q-1) = \phi(r)$ , ki pa ga ne vemo, če ne poznamo razcepja r.



## WILSONOV IZREK

$n \in \mathbb{N}$  je praštevilo  $\Leftrightarrow (n-1)! \equiv -1 \pmod{n}$

D: ( $\Leftarrow$ ): Če  $n$  ni praštevilo, je deljivo z mestom  $m$ ,  $1 < m < n$ .

Tetja  $(n-1)! \equiv 0 \pmod{n}$ . Ena od lastnosti homogenec:

$a \equiv b \pmod{n}$  in  $d | n \Rightarrow a \equiv b \pmod{d}$ ,ato bi moralo iz

$(n-1)! \equiv -1 \pmod{n}$  slediti  $(n-1)! \equiv -1 \pmod{m}$ . A vemo, da

$0 \equiv -1 \pmod{n}$ .  $\rightarrow \Leftarrow$

$$\rightarrow a-b = k \cdot m = k \cdot d \cdot l \Rightarrow a \equiv b \pmod{d}$$

( $\Rightarrow$ ): Posebij za  $p=2$ :  $1! \equiv 1 \equiv -1 \pmod{2}$  ✓ Zdaj je  $p$  lahko

praštevilo. Po matem Fermatovem izreku je  $x^{p-1} \equiv 1 \pmod{p}$

za vsake  $x \in \mathbb{Z}$ , ki ni homogenec  $p$ . Torej ima polinom

$g(x) = x^{p-1} - 1 \pmod{p}$  nihče  $1, 2, 3, \dots, p-1$ . Tudi polinom

$h(x) = (x-1)(x-2) \dots (x-(p-1))$  ima nihče  $1, 2, \dots, p-1$ . Cilide na

modul  $p$  sta  $g$  in  $h$  enaka. Če vstavimo motor  $x=0$ ,

dobimo  $g(0) \equiv -1 \pmod{p}$  in  $h(0) = (-1)(-2) \dots (-p+1) \pmod{p}$

Ker  $p$  je lahko, je neden minusor in  $h(0) = (p-1)! \pmod{p}$ .

$$(p-1)! \equiv -1 \pmod{p} \blacksquare$$



## OSNOVNE LASTNOSTI IN PORAZDELITEV PRAŠTEVIL

Praštevilo je m ∈ N, ki ima natančno dva delitelja: 1 in samega sebe.

Praštevil je neskončno mnogo.

Euklidov dokaz: Če bi bila močica praštevil  $\{p_1, p_2, \dots, p_k\}$  končna, bi bilo število  $n = p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$  sestavljeno, torej deljivo z vsej enim praštevilm  $p_i$ . Velja  $n \equiv 1 \pmod{p_i}$  za vsak  $i=1, \dots, k$ , to je  $\rightarrow$

2 je sodo praštevilo; ostala so liha. Toračen 2 in 3 so oblike  $6k+1$  ali  $6k-1$  za  $k \in \mathbb{N}$ . Eratostenovo rešitev.

Odprt problem: ali obstaja neskončno praštevilske dvojčke?

Fermatova števila  $f_n = 2^{2^n} + 1$  niso vsa praštevila, so pa vsa paroma tudi  $\rightarrow$  spet dolar za neskončnost praštevil.

Mersenova števila  $M_n = 2^n - 1$  so lahko praštevila, če je n praštevilo.

Največja znana praštevila so Mersenova.

$\pi(x) =$  število praštevil, manjših od x

Eulerjeva ocena  $\pi(x) \geq \ln x - 1$ . Če bi približno veljala, bi bilo praštevil sorazmerno množ. Eulerjev izrek  $\sum_{p \in \mathbb{P}} \frac{1}{p} = \infty$ , to pa pomeni, da jih je kar veljav.

• Obstajajo poljubno dolgi oddeli naravnih števil, na katerih ni praštevila, npr.  $N =$  produkt vseh praštevil do n,  $N+2, N+3, \dots, N+m$  je zaporednih  $n-1$  sestavljenih števil.

$\pi(x) \sim \frac{x}{\ln x}$ ,  $\pi(x) \sim \int_2^x \frac{dt}{\ln t}$  f  $\sim g$  pomeni  $\lim_{x \rightarrow \infty} \frac{f(x)}{g(x)} = 1$  (dimo povečevanje)

Izraz aritmetično zaporedje  $a+nb$  za  $(a, b)=1$  vsebuje neskončno praštevila. (dimo povečevanje doljca)



## VSOTE DVEH KVADRATOV

Kvadrat soden je  $\equiv 0 \pmod{4}$ , kvadrat libega  $(2k+1)^2 \equiv 1 \pmod{4}$ , zato je vsota dveh kvadrator po mod 4 enaka  $0+0, 0+1, 1+1 \pmod{4}$  ali 2.

$\Leftrightarrow$  je  $n \equiv 3 \pmod{4}$ , se n ne da zapisati kot vsota dveh kvadrator celih števil. Če velikostih drugih se ne da.

Končni rezultat: število  $n \in \mathbb{N}$  je izrazljivo kot vsota dveh kvadrator celih števil  $\Leftrightarrow n$  pravstevljšem razcepnu za n nastopajo vse pravstevila, kongruentna  $3 \pmod{4}$ , s sodimi potencami.  $n = (p_1^{t_1} \dots p_k^{t_k})^2$  gde je  $= (p_1^{t_1} \dots p_k^{t_k})^2 a^2 + (p_1^{t_1} \dots p_k^{t_k})^2 b^2$ , torej pravstevila na sode potence lepo izpostavimo. Istance produkt različnih pravstevil.

$\Leftrightarrow$  sta m in n vsoti dveh kvadrator, je tudi njun produkt.

$$m = x^2 + y^2 = \| (x+iy) \|^2, \quad n = u^2 + v^2 = \| (u+iv) \|^2, \quad m \cdot n = \| (x+iy)(u+iv) \|^2 =$$

$$= (ux - vy)^2 + (xv + yu)^2.$$

Zdaj nas ramina le že vralo posamezno pravstevilo.  $2 = 1^2 + 1^2$ .  $p \equiv 3 \pmod{4}$  se ne da. Tako  $p \equiv 1 \pmod{4}$  se da zapisati kot vsoto kvadrator celih števil. To je

takoj, ko ima kongruenca  $-1 \equiv m^2 \pmod{p}$  dve rešitvi.

(Pravz dolg rezultaten dolazek.)

## IZREK O VSOTI ŠTIRIH KVADRATOV



Ustavo naravno število se da napisati kot vsota štirih kvadratov celih števil. (Kot pri vsoti dveh kvadratov tudi tuhaj dopuščamo ničle.)

Če sta  $m, n \in \mathbb{N}$  predstavljeni kot vsoti 4 kvadratov celih števil, je tudi njun produkt mogočno predstaviti v takih oblikah. Gremo v kvaternione  $\mathbb{H}$ . (Ni kompl.)

$$\alpha = x + iy + jz + kw \quad \alpha^* = x - iy - jz - kw \quad i^2 = j^2 = k^2 = ijk = -1$$
$$N(\alpha) = \alpha\alpha^* = x^2 + y^2 + z^2 + w^2 \quad \text{in} \quad N(\alpha\beta) = \alpha\beta\alpha^*\beta^* = \alpha\beta\beta^*\alpha^* =$$
$$= \alpha N(\beta)\alpha^* = N(\alpha)N(\beta)$$

Ustavo prastevilo je izrazljivo kot vsota štirih kvadratov celih števil.  $2 = 1^2 + 1^2 + 0^2 + 0^2$ .

Za loko prastevilo  $p$  obstaja  $t < p$ , da je  $tp$  vsota štirih kvadratov.  $S = \{0, 1, \dots, \frac{p-1}{2}\}$  da vse možne kvadrate mod  $p$ , esto  $\{x^2(p) | x \in S\}$  in  $\{-1 - y^2(p) | x \in S\}$  dosta  $\frac{p+1}{2}$  različnih elementov, torej je  $\frac{p+1}{2} \cdot 2 = p+1$  in obstajata  $x, y$ , da je  $x^2 \equiv -1 - y^2 \pmod{p} \Rightarrow x^2 + y^2 + 1 \equiv 0 \pmod{p}$ ,  $x^2 + y^2 + 1 = tp$ ,  $x, y \leq \frac{p}{2} \Rightarrow tp = x^2 + y^2 + 1 \leq \frac{p^2}{4} + \frac{p^2}{4} + 1 = \frac{p^2}{2} + 1 < p^2 \Rightarrow t < p$ .

Loko prastevilo je izrazljivo kot vsota štirih kvadratov.

Obstaja  $t < p$ , da  $tp = x^2 + y^2 + z^2 + w^2$ . Želimo najmanj tak t. V primeru t je red in v primeru t lahko  $\geq 3$  dobimo protislogi s minimalnoštej t.



# VERIŽNI ULOMKI

$$\frac{a}{b} = [q_1, q_2, \dots, q_{n+1}] = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \dots + \frac{1}{q_{n+1}}}}$$

$q_i$  dolino s pomočjo

Euklidovega algoritma.

$$r_{-1} = a = q_1 b + r_1$$

$$r_0 = b = q_2 r_1 + r_2$$

$$r_n = q_{n+1} r_{n-1} + r_n$$

$$x_{i+1} = x_{i-1} + q_{i+1} x_i \quad x_{-1} = 1 \quad x_0 = 0$$

$$y_{i+1} = y_{i-1} + q_{i+1} y_i \quad y_{-1} = 0 \quad y_0 = 1$$

$$r_i = (-1)^{i-1} x_i a + (-1)^i y_i b$$

$$\frac{15}{4} = 3 + \frac{3}{4} = 3 + \frac{1}{\frac{4}{3}} = 3 + \frac{1}{1 + \frac{1}{3}} = 3 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1}}} = [3, 1, 3]$$

$$\frac{15}{4} = 3 + \frac{3}{4} = 3 + \frac{1}{\frac{4}{3}} = 3 + \frac{1}{1 + \frac{1}{3}} = 3 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1}}} = [3, 1, 2, 1]$$

Vsek  $r \in \mathbb{Q}$  lahko narišemo s končni enostavnimi verižnimi ulomki  $r = [q_1, \dots, q_n]$ ,  $q_i \in \mathbb{Z}$ ,  $q_i \in \mathbb{N}$ . Imamo enotičnost, ker je ip na zadnjem mestu 1, ip lahko pristojeno pred zadnjemu mestu. Bježiš  $\mathbb{Q}$  in verižni ulomki  $\approx 2^{m/2}$ .

Verižni ulomki lahko seznamo tudi druga števila, a tam ni enotičnosti.  $[1, -\sqrt{2}, 1, \sqrt{2}]$

i-ti konvergent verižnega ulomka  $c = [q_1, \dots, q_n]$  je

$$c_i = [q_1, \dots, q_i]. \quad T: c_i = [q_1, \dots, q_i] = \frac{y_i}{x_i}, \text{ kjer je}$$

$$x_i r_1 = x_{i-1} + q_{i+1} x_i, \quad y_{i+1} = y_{i-1} + q_{i+1} y_i, \quad y_{-1} = 0 \quad y_0 = 1.$$

D: indukrip... T: Vsi konvergenti so okrajeni ulomki.  $d(x_i, y_i) = 1$

Dolino rešitev diophantske enačbe:  $\frac{a}{b} = [q_1, \dots, q_n]$ ,  $\frac{a}{b} = c_n = \frac{y_n}{x_n}$ ,

$$\cancel{\frac{a}{b}} y_{n-1} - \cancel{\frac{a}{b}} x_{n-1} = (-1)^{m-1} \quad (\text{Enačba je rešljivome enačba})$$

$$x_i y_{i-1} - y_i x_{i-1} = (-1)^{i-1}, \quad x_i y_{i-2} - y_i x_{i-2} = (-1)^i q_i. \quad \text{Roktor DE}$$

$a x + b y = 1$  dolino je predradnje konvergente.

Velikost konvergentov (končnega) enostavnega verižnega ulomka:  $c_1 < c_3 < c_5 < \dots \leq c \leq \dots < c_6 < c_4 < c_2$ .

$c_i = \frac{y_i}{x_i}$  imenovalci naravajo:  $x_{i+1} > x_i$



## IZREK O NAJBOLJŠI APROKSIMACIJI

T: Za poljubno iracionalno število  $\gamma$  obstaja natančno en mestnoučni verižni ulomek  $[g_1, g_2, g_3, \dots]$ , ki je enak  $\gamma$ . Konvergenti  $c_i$ : bili naravčajo, sodi podajo  $c_1 < c_3 < \dots < c_4 < c_2$  in limita je ista, naj  $c_{i+1} - c_i = \frac{(i-1)^{i-1}}{x_{i-1} x_i}$  in  $x_i$  naravčajo po velikosti.

$$\text{Primer: } \gamma = \sqrt{7} \quad g_1 = \lfloor \sqrt{7} \rfloor = 2 \quad g_2 = \lfloor \frac{1}{\sqrt{7}-2} \rfloor = \lfloor \frac{\sqrt{7}+2}{3} \rfloor = 1$$

$$g_3 = \lfloor \left( \frac{\sqrt{7}+2}{3} - 1 \right)^{-1} \rfloor = \lfloor \frac{3}{\sqrt{7}-1} \rfloor = \lfloor \frac{\sqrt{7}+1}{2} \rfloor = 1 \quad g_4 = \lfloor \left( \frac{\sqrt{7}+1}{2} - 1 \right)^{-1} \rfloor = 2$$

$$= \lfloor \frac{2}{\sqrt{7}-1} \rfloor = \lfloor \frac{\sqrt{7}+1}{3} \rfloor = 1 \quad g_5 = \lfloor \dots \rfloor = \lfloor \sqrt{7}+2 \rfloor = 4 \quad g_6 = \lfloor \frac{1}{\sqrt{7}-2} \rfloor = 1 \stackrel{\text{se zanje}}{\leftarrow} \stackrel{\text{ponavljati}}{\Rightarrow}$$

$$\sqrt{7} = [2, \overline{1, 1, 1, 4}] \quad \text{Približki: } c_1 = \lceil 2 \rceil = 2, \quad c_2 = \lceil 2, 1 \rceil = 2 + \frac{1}{1} = 3,$$

$$c_3 = 2 + \frac{1}{1+1} = 2,5 \quad c_4 = 2 + \frac{1}{1+\frac{1}{1+1}} = 2 + \frac{2}{3} = 2,66, \quad$$

$$c_5 = \lceil 2, 1, 1, 1, 4 \rceil = \lceil 2, 1, 1, \overline{\frac{5}{4}} \rceil = \lceil 2, 1, \overline{\frac{9}{5}} \rceil = \lceil 2, \overline{\frac{14}{9}} \rceil = \frac{2 \cdot 14 + 9}{9} = \frac{37}{9} = 2,6444 \dots$$

Konvergenti verižnega ulomka za iracionalna števila so najboljši racionalni približki tega števila z dano velikostjo imenovalca.

T:  $\gamma = [g_1, g_2, \dots]$  in  $\frac{a}{b} \in \mathbb{Q}$  obrajen. Če je  $|\gamma - \frac{a}{b}| < |\gamma - \frac{y_i}{x_i}|$ , potem je  $b > x_i$ . Če je  $|b\gamma - a| < |x_i\gamma - y_i|$  za  $i \geq 1$ , je  $b > x_{i+1}$  v tem primeru.

I: Naj bo  $\gamma$  iracionalno št. in  $\frac{a}{b} \in \mathbb{Q}$ , da je  $|\gamma - \frac{a}{b}| < \frac{1}{2b^2}$ . Potem je  $\frac{a}{b}$  konvergent enostavnega verižnega ulomka za  $\gamma$ . To je super približek.

# PERIODIČNI VERIŽNI ULOMKI



Kvadratično število je število, ki je rešitev kvadratne enačbe s celimi koeficienti. Obliko  $\frac{a+\sqrt{b}}{c}$ ,  $a \in \mathbb{Z}, c \in \mathbb{N}$

Če je  $\delta = [\underline{g_1, g_2, \dots, g_n}]$  čisto periodični verižni ulomek, dobimo kvadratno enačbo za  $\delta = [\underline{g_1, \dots, g_n, \delta}]$ , zato je  $\delta$  kvadratično število. Tudi v primeru  $\gamma = [r_1, \dots, r_m, \delta]$  je  $\gamma$  kvadratično, saj lahko razširimo verižni ulomek in dobimo spet obliko  $\frac{a+\sqrt{b}}{c}$ .

1. Vrsto kvadratično iracionalno število ima periodični verižni ulomki. Biježija periodični verižni ulomki  $\leftrightarrow$  kvadratična iracionalna števila. Zvod konvergenčnih dolgor

Zlati raz.  $\gamma = [1, x] \quad \frac{1+x}{x} = \frac{x}{1} \quad 1+x=x^2 \rightarrow x=1+\frac{1}{x}= [1, x]$

Zlati razmerje  $x = \frac{1+\sqrt{5}}{2}$  je "najbolj iracionalno število" s verižnim ulomkom  $[1, 1, 1, 1, \dots]$ .

Kvadratično iracionalno število  $\gamma$  ima povsem periodični verižni ulomki  $\Leftrightarrow \gamma > 1$  in  $\gamma^* \in (-1, 0)$ .

Število  $\gamma = [\underline{\overline{f_m}}] + \overline{f_m} > 1$  in  $\gamma^* \in (-1, 0)$  ima povsem periodičen verižni ulomek  $\Rightarrow \gamma = [\underline{g_1, \dots, g_n}]$  in  $\overline{f_m} = [\underline{L_i \overline{f_m}}, g_{i+1}, \dots, g_n, 2L_i]$

T: Naj bo  $n \in \mathbb{N}$  nekvadrat, k  $k$  minimalna perioda verižnega ulomka za  $\overline{f_m}$  in  $\frac{y_i}{x_i}$  i-ti konvergent za  $\overline{f_m}$ . Potem je  $y_{k+1}^2 - n x_{k+1} = (-1)^{k+1}$  za  $\forall k \in \mathbb{N}$ . Če je k sodna perioda, je osnova rešitev Pellove enačbe  $(x_k, y_k)$ , sicer pa  $(x_{2k}, y_{2k})$ .

# PELLOVA ENAČBA



$$y^2 - mx^2 = 1, \text{ menjam, iščemo } x, y \in \mathbb{Z}.$$

Tedno rešitev  $y=1, x=0$ . Če je  $(x,y)$  rešitev, tudi  $(x,-y), (-x,y), (-x,-y)$ .

Če je  $n$  popolni kvadrat, je le trivialna rešitev, saj lahko razstavimo  $y^2 - mx^2 = (y-mx)(y+mx) = 1 = 1 \cdot 1$ .

Zanimiva nas pa je  $m$  nekvadrat. Z enačbo so se ulevajali če starički,

ker da zelo dober približek za koncne:  $y^2 - mx^2 = 1 / :x^2$

$$\left(\frac{y}{x}\right)^2 = m + \frac{1}{x^2} \quad \frac{y}{x} = \sqrt{m}$$

$$y^2 - mx^2 = (y + x\sqrt{m})(y - x\sqrt{m})$$

$\cap \mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\}$  upoštevamo konjugiranje  $z^*$ :

$$(a + b\sqrt{m})^* = a - b\sqrt{m} \quad N(z) = N(a + b\sqrt{m}) = z z^* = (a + b\sqrt{m})(a - b\sqrt{m}) = a^2 - mb^2.$$

Rešitve Pellove enačbe imajo normo 1. Rešitve lahko množimo med seboj. Poisciemo najmanjšo nemivialno rešitev in jo

potenciramo. Vse rešitve Pellove enačbe  $y^2 - mx^2 = 1$ , ki ustrezajo  $y + x\sqrt{m} > 0$ , so oblike  $(x_k, y_k)$ , kjer je  $y_k + x_k\sqrt{m} = (b + a\sqrt{m})^k$ ,  $k \in \mathbb{Z}$  in je  $(a, b)$

najmanjša naravna rešitev. D: Če bi obstajala ena,

ki ni potenca  $(b + a\sqrt{m})$ , je med sredina:  $(b + a\sqrt{m})^k < (b + a\sqrt{m})^{k+1}$ ,

množimo z  $(b - a\sqrt{m})$  in dobimo  $1 < (b + a\sqrt{m})(b - a\sqrt{m})^k < b + a\sqrt{m}$ , kar je

→ v tem, da je  $(a, b)$  najmanjša naravna rešitev. ■

Naravna rešitev  $(x,y)$  je zelo dober približek za  $\sqrt{m}$ :  $| \frac{y}{x} - \sqrt{m} | < \frac{1}{2x^2}$

$$| \frac{y}{x} - \sqrt{m} | = \frac{| y - x\sqrt{m} |}{x} = \frac{1}{x(y + x\sqrt{m})} < \frac{1}{x(x\sqrt{m} + x\sqrt{m})} < \frac{1}{2x^2} \quad \forall n > 1$$

• Edaj pripeljmo ora teorijo rešitev ulomkov (glej prejšnjo stran.)